

1. In your report, you state that *“it is of concern to the SIAT that Safety and Mission Assurance did not directly brief the SIAT and had little visibility throughout the assessment. Of greater concern is that the performance of Safety and Mission Assurance duties appear to be diminishing.”*

- 1a. To what do you attribute the diminution of the role of Safety and Mission Assurance in the Shuttle program?

The Shuttle is a complex, well-defended, yet aging system that operates in an unforgiving flight environment and requires extensive, often intrusive maintenance. In its review, the SIAT observed an “erosion” of some Shuttle safety-critical defenses, including those associated with the Safety and Mission Assurance function. The SIAT attributed this erosion to several factors. Those specific to diminution of the performance of Safety and Mission Assurance duties include:

- the desire to “streamline” Shuttle operations with accompanying reduction of resources and staff, and elimination of numerous Government Mandatory Inspection Points;
- “success-engendered safety optimism,” which refers to the tendency to accept risk based on past success without rigorous analysis and understanding, and fosters complacency in problem reporting and investigation;
- the perception that the Shuttle is now an “operational” rather than an experimental vehicle, which promotes the use of fair wear and tear allowances, standard repairs, and self-inspection;
- the change in role from one of “oversight” to one of “audit” as Shuttle operations were transitioned to a contractor force.

- 1b. In your opinion, what would need to be done to restore the Safety and Mission Assurance function to its appropriate status?

As the causal factors above indicate, the erosion of the Safety and Mission Assurance function is related to conditions internal and external to its organization. The SIAT believes the Safety and Mission Assurance requires strengthening from within as well as increased attention from the Shuttle Program itself.

From Within: The S&MA function needs to be strengthened by adding and developing system experts and technical leaders who are proactive in measuring and assessing system condition and state, investigating problems, and advising program management, rather than reactive in providing policy and auditing compliance. This would require additions to resources and technical staffing, and just as critical, a cultural change.

Externally: To guard against the tendency toward casual risk acceptance, the Program should return to treating the Shuttle as an experimental vehicle. Further,

the “Safety First” message needs to be emphasized by actions rather than diluted by stream-lining directives. Such actions should include renewed focus on addressing open waivers and CAR’s (Corrective Action Reports), requiring root cause determination, and assessing relaxation of standards (e.g. Fair Wear & Tear, “in family” vs. “out of family” problems, etc.).

- 2. Your report states that the safety support contractor at the Marshall Space Flight Center reduced its staffing from 150 to 80 (about a 53% reduction) in 1995. Did anyone explain to your team why this critical function was required to take such a significant cut?**

The primary reason given to the SIAT for the reduction in staff was a “consolidation of contracts” that began around 1994. Prior to this time, support service contractors supported the Safety and Mission Assurance function at Marshall with problem reporting and resolution. During the contract merger, several deliverables, including numerical trending of SSME problems, were dropped. Although not explicitly stated, it was assumed that the reduction was related to a projected decrease in workload associated with the effort to streamline the Shuttle program.

- 3. You noted in your report that “*This lack of statistical risk assessment is almost cultural.*” You also noted that there is heavy reliance on redundancy as a means of mitigating risk. What would be required in order to improve the current Quantitative Risk Assessment System (QRAS) model to make it acceptable to Shuttle managers, and are there ways that its deployment could be expedited?**

The Shuttle Program has historically relied on qualitative risk identification methods to guide the design, testing, and inspection requirements for Shuttle systems. It was apparent to the SIAT that the Program resistance to quantitative analysis stems from the view that such methods are extremely time- and resource-intensive, and still mostly subjective. Further, managers find point estimates of failure probability difficult to interpret and utilize without additional decision analysis support.

QRAS is an attempt to facilitate probabilistic risk assessment for the Shuttle by incorporating risk models that can be readily accessed by engineers to build event and fault trees. Subjectivity is still a limitation in QRAS given the use of expert opinion to determine probabilities of occurrence and the use of standard risk analysis methods (e.g., Fault Tree Analysis) that rely on the analyst to select the relevant initiating events. QRAS also does not utilize decision theory to assist decision-makers in evaluating alternatives or resolving conflicting goals.

The SIAT did not perform a detailed review of the adequacy of the QRAS model. However, a recent review of the implementation of current technologies in QRAS conducted by experts in the field of probabilistic risk assessment found it to be problematic. Reasons provided in the January, 2000 report include:

- There is no common overarching system model to guide scenario generation and causal modeling.
- Analysis modules artificially isolate failure modes from other modes and scenarios.
- Scenario development suffers from insufficient considerations of intermediate events (e.g., SSME engine shutdown is perfectly executed).
- Uncertainties are treated inconsistently or not at all.
- It does not explicitly include human process error in risk models, nor does it consider risks generated by the organization structure.

While QRAS was not examined in-depth, the SIAT did investigate the effectiveness of the problem reporting and corrective action (PRACA) system used by the Shuttle Program. PRACA was found to contain a number of serious deficiencies. Because the usefulness of QRAS assessment can only be as good as the data used to determine probabilities and actual failure modes, significant improvements to PRACA need to accompany any QRAS deployment effort.

As stated in the report, the SIAT believes that in its current state QRAS should be used with caution. It must be thoroughly validated and its deficiencies corrected before deployment. Assigning a single, core team of experts to lead the QRAS development will facilitate deployment. The Shuttle Independent Assessment Team has also made a number of recommendations for improving risk management within the Shuttle program that should be addressed.

4. The SIAT report (e.g., Finding no. 1 in the Risk Assessment and Management section) indicates that the Shuttle program may be working with optimistic or inaccurate evaluations of risk. Given that finding, how confident are you that the quantitative risk reduction estimates associated with proposed safety upgrades are accurate?

The SIAT did not directly or extensively address Shuttle upgrades (reference Issue 9 in Executive Summary of the report) and cannot comment on the *accuracy* of these specific risk reduction estimates. However, to the extent that the SIAT is aware of the upgrades selected, it believes that the Probabilistic Risk Assessments (PRA's) and Failure Mode and Effects Analysis (FMEA's) performed have consistently identified high-risk elements that should be addressed and views the risk reduction estimates as relative rather than absolute numbers. Precision in the point estimates of risk may not be necessary if leading risk contributions are clear and not sensitive to the analysis methods.